DOI 10.29042/2019-5004-5008

Helix Vol. 9 (3): 5004- 5008

Image Tampering Detection Techniques: A Statistical Review

*[1]Sonal Patil, [2]Dr. K. N. Jariwala

[1]Ph.D. Research Scholar, Computer Engineering Department, S.V.N.I.T, Surat

[2]Assistant Professor, Computer Engineering Department, S.V.N.I.T, Surat

*Email: sonalpatil3@gmail.com, knj@coed.ac.in

Received: 26th December 2018, Accepted: 13th February 2019, Published: 30th June 2019

Abstract

Copyrights and digital signatures have boosted a wide variety of research areas in image security domain. Even though these systems are very secure, but there exists a gap between copyrighting an image, and an attacker actually using the image for their own purposes. Usually attackers will try to remove or alter with the original signatures present in the image, and thereby there is a need of forgery detection algorithms in order to track the validity of the image under test. In this paper we provide a statistical review of various algorithms used to detect forgery of images, and focus on algorithms which have good accuracy of forgery detection upon comparison

Keywords

Forgery, Copyright, Signature, Attacker, Authenticity

Introduction

Image forgery detection has been a topic of research for more than 2 decades now, it includes multiple levels of processing for the input image. These levels are depicted with the help of figure 1 as follows,

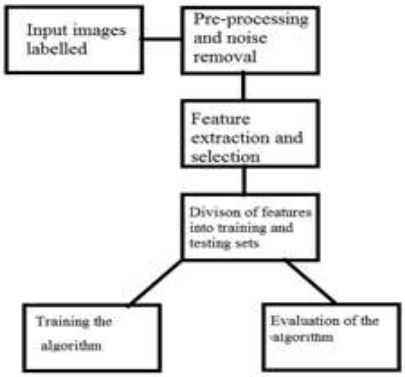

Figure 1: Flow of Image Forgery Detection

The info pictures can be forged pictures, non-forged pictures, the stream dependably stays steady. The pictures are gathered and named by the classes required at the yield. For instance, for forgery discovery, we require the yield to contain classes like typical, grafting forgery, duplicate move forgery among others, so we gather pictures and name them with the given classes, this progression is basic, and characterizes the precision of the general forgery recognition process, a completely chose dataset guarantees better characterization results. The gathered pictures are then given to a pre-handling and commotion evacuation square, where the pictures are cleaned of any clamors and are prepared so they are prepared for highlight extraction. The handling incorporates, picture combination, division of the picture, and any morphological structure tasks on the picture, among different advances which are typically dataset subordinate. Some datasets don't require clamor evacuation, while others do, along these lines this progression is generally chosen according to the application originator's need. The prepared picture is then given to the element extraction unit, where the highlights of the picture are assessed. Highlight assessment is another exceptionally basic advance, it characterizes the exactness with which highlights are assessed for the picture, numerous strategies including Speed up Robust Features (SuRF) and others have been proposed explicitly for forgery recognition so as to have better element extraction ability. Highlight assessment is typically gone with highlight determination for expansive datasets, so as to expel any repetition from the separated highlights. After component extraction, the forgery discovery classifier is prepared with the information highlights, preparing is finished with the pictures removed from the preparation set, while the genuine forgery recognition is done from the assessment square, where the prepared classifier is utilized with the information highlights from the given picture. The preparation and testing

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

(assessment) sets are chosen dependent on the application, normally 70% of the information is utilized for preparing, while at the same time staying 30% of the information is utilized for assessment. The assessment procedure distinguishes the exactness of the classifier utilized for the procedure, and can be utilized to re-train the calculation so as to enhance the precision dependent on the means pursued by the framework.
In this paper, we have compared various algorithms for forgery detection, and identified the optimum algorithms used for a given application; the next section describes the algorithms in brief, followed by the comparison of results between the algorithms. Finally we conclude the paper with some interesting observations about the compared algorithms and proposed the future work which researchers can perform in order to further analyze these algorithms.

Literature Review

Advanced picture forgery recognition systems are assembled into two classes, for example, dynamic methodology and uninvolved methodology. In the dynamic methodology, the watermarked image is implanted with the given data. Special cameras are needed for this purpose as watermark is implanted at the source itself. No implantation is needed in latent methodology, as this strategy works simply by breaking down the twofold data of a picture. Inactive picture forgery location procedures generally gathered into five classes,

1. Pixel-Based Picture Forgery Location

Pixel-put together systems emphasize the input image with respect to the gray levels. There are 4 kinds of systems for this, which are, duplicate move, joining, resampling and factual. All these strategies are useful for detecting modern day forgeries in images

2. Arrangement Based Picture Forgery Recognition

Another type of forgery detectors are called as arrangement based detectors. Picture groups are the main application of this method, like the methods of Joint Photographic Expert Group (Joint picture exchange group FORMAT). Factual relationship presented by explicit lossy pressure plans, which is useful for picture forgery location. These methods can be apportioned into three sorts, which are majorly based on qualtization and blocking of Joint picture exchange group FORMAT structure. These methods work even if the picture is compressed or compacted.

3. Capture Device Based Picture Forgery Recognition

At whatever point we snap a photo from an advanced camera, the pixels gets transferred from the lens to the memory with various operations being performed on it, which include levelization, shading relationship, gamma revision, white changing, sifting, and compression using Joint picture exchange group FORMAT. These preparing ventures from catching to sparing the picture in the memory may move on the commence of camera model and camera collectibles. These strategies take a shot at this standard. These strategies can be isolated into four classes, for example, chromatic abnormality, shading channel exhibit, camera reaction and sensor disruptions.

4. Physical Condition Based Picture Forgery Identification

These strategies fundamentally dependent on three dimensional connections between physical question, light and the camera. Consider the production of a forgery demonstrating two film stars, reputed to be impractically included, walking around a dusk shoreline. Such an image might be made by joining together individual photos of every motion picture star. As such, it is much of the time hard to precisely coordinate the lighting impacts under which every individual was at first caught. Complexities in lighting over a picture can be used as verification of changing. These procedures take a shot at the dependence of the lighting condition under which an article or picture is gotten. Lighting is the most essential factor for catching a picture. These systems are secluded into three characterizations, based on the light bearing capacity of the camera which can be 2D or 3D.

5. Geometry-Based Picture Forgery Location

These systems fundamentally dependent on primary point which depends on the direction of the camera focus onto the picture plane, which makes estimation of the question on the planet and their position with respect to camera. Equipments for image capture made in gun barrels give a wind onto the shot for expanded exactness and range. These equipments for image capture familiarize somewhat specific markings to the shot discharged, and can subsequently be used with a specific handgun. In a similar sense, a few picture scientific strategies have been created that especially show relics introduced by various periods of the imaging strategy. Geometry-based picture forgery recognition techniques are isolated into two classes, for example, rule point and metric estimation

Figure 1 shows the basic framework for forgery detection [2]. Fridrich et al. [20] proposed a technique for distinguishing copymove picture forgery in 2003. In this strategy, the picture is isolated into covering squares (16 x16), and Discrete cosine transform coefficients are utilized for highlight extraction of these squares. By then, the Discrete cosine transform coefficients of squares are lexicographically arranged. After lexicographical arranging, tantamount squares are recognized and forged locale is found. In this paper the developers of the technique perform hearty modifying tasks in the picture. Be that as it may, the developers of the technique have not played out some other power test. Popescu et al. [21] proposed a strategy for recognizing copy picture

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

locales in 2004. In this technique, the developers of the technique connected PCA on settled size picture of square size (16 x 16, 32 x 32), at that point registered the Eigen esteems and eigenvectors of each square. The copy areas are consequently recognized by utilizing lexicographical arranging. This calculation is a proficient and hearty strategy for picture forgery identification regardless of the picture type. Kang and Wei [8] have used Singular Value Decomposition to recognize the modified territories in a computerized picture in 2008. In this paper Authors used Singular Value Decomposition for separating highlight vector and measurement decrease. Comparable squares are recognized by utilizing lexicographical arranging on line and section vectors and to identify forged districts. This technique is powerful and effective. Lin et al. [15] proposed fast duplicate move forgery identification strategy in 2009. In this paper Authors used PCA for discovering highlights vectors and measurement decrease after that Radix sort is connected on highlight vectors to perceive fake. This calculation is capable and works honourably in uproarious and compacted pictures. Huang et al. [9] proposed duplicate move forgery recognition in advanced pictures utilizing Scale invariant fourier transform calculation in 2009. In this paper, the developers of the technique displayed SCALE INVARIANT FOURIER TRANSFORM estimation calculation utilizing highlight coordinating. This calculation gives extraordinary outcomes notwithstanding when picture is packed or boisterous. Li et al. [10] proposed a duplicate move forgery discovery dependent on arranged neighbourhood approach by utilizing Discrete wavelet transform and SINGULAR VALUE DECOMPOSITION in 2007. In this paper, The developers of the technique used Discrete wavelet transform and broke down into four sub-gatherings. SINGULAR VALUE DECOMPOSITION was used in low-recurrence sub bands for measurement decrease. By then, they associated lexicographical arranging on specific quality vector and the forged district is perceived. They attempted this calculation for grayscale and shading pictures. This calculation is strong. Luo et al. [16] proposed a solid ID of copied area in advanced pictures in 2006. In this paper, the developers of the technique separate a picture into covering squares and after that apply closeness coordinating calculation on these squares. The comparability coordinating calculation perceives the duplicate move forgery in the given picture. This technique also meets desires in the Joint picture exchange group FORMAT pressure, added substance commotion and Gaussian obscuring. Zhang et al. [17] proposed another strategy for cop-move forgery recognition in advanced picture in 2008. The developers of the technique used Discrete wavelet transform and separation given picture into four non-covering sub images and stage connection is received to figure the spatial balance between the duplicate move forgery areas. By then, they connected closeness coordinating calculation between the gray levels for recognizing forged districts. This technique capacities commendably in the very packed picture and amazingly powerful with lower computational time as contrasted and different strategies. Kang et al. [18] proposed a strategy to recognize duplicate move forgery in computerized picture in 2010. In which right off the bat picture is partitioned in sub-squares at that point connected enhanced SINGULAR VALUE DECOMPOSITION on every square. By then, closeness coordinating is performed on every square dependent on the lexicographically arranged SV vectors. Finally the regions of forgery are detected. Researchers in the work done in [11] proposed a technique to distinguish copy move forgery dependent on Discrete wavelet transform-Discrete cosine transform (QCD) in 2011. The developers of the technique used Discrete wavelet transform to separate picture into sub-groups, at that point performed Discrete cosine transform-QCD (Quantization coefficient deterioration) in line vectors to decrease vector length. Move vector is processed after lexicographically arranging of the line vectors, at that point it is contrasted and edge lastly copied locale of a picture is featured. The work given in [6] proposed a calculation to identify grafting picture forgery with viewable signs in 2009. The developers of the technique utilized a recognition window and separated it into nine sub-squares. VAM (visual thought show) is utilized to recognize a fixation point and a short time later element extraction is utilized to separate the joined locale in the computerized picture. Similarly in [19] the researchers had proposed a programmed and speedy changed Joint picture exchange group FORMAT picture recognition strategy utilizing examination of Discrete cosine transform coefficient in 2009. The developers of the technique have used Discrete cosine transform coefficient and Bayesian methodology for highlight extraction, at that point comparability coordinating calculation is utilized to distinguish copied area outline. Another work in [19] proposed a technique to recognize duplicate move forgery dependent on Improved Discrete cosine transform of a picture in 2011. In this paper, Discrete cosine transform coefficients are utilized for discovering highlight vector. After that similitude coordinating calculation is utilized to recognize impersonation territories of a picture. Even in [18] the researchers proposed a vigorous calculation to identify copymove forgery in advanced picture in 2012. In this paper, The developers of the technique have utilized Discrete cosine transform for discovering Discrete cosine transform coefficients of each square that are spoken to by circle square and concentrate highlight from each circle square, at that point seeking task is performed to discover comparable square combines for copied area outline. An interesting research shown in [14] proposed a visually impaired duplicate move picture forgery location strategy utilizing dyadic wavelet change (DyWT). DyWT is move invariant and consequently more pertinent than Discrete wavelet transform for information investigation. In this strategy First we deteriorate the information picture into estimate (LL1) and detail (HH1) subbands. At that point we partition LL1 and HH1 subbands into covering squares and measure the comparability between squares. The principle thought is that the comparability between

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

the duplicated and moved squares from the LL1 subband ought to be high, while the one from the HH1 subband ought to be low because of clamor irregularity in the moved square. This strategy isn't significant for shading data as opposed to changing over the shading pictures to dim pictures. This technique is very effective strategy Another research in [15] proposed a technique to recognize Copymove forgery, which is one sort of hardening that is generally utilized for controlling the computerized pictures. In this strategy a piece of a picture is replicated and is glued on another locale of the picture. In this work proficient non-meddlesome strategy for duplicate move forgery location is clarified. This strategy depends on picture division and similitude location utilizing dyadic wavelet change (DyWT). Reordered areas are fundamentally comparable and this basic similitude is distinguished utilizing DyWT and factual measures. The outcomes demonstrate that this technique outflanks the detail of-the workmanship strategies. In this paper calculation adequately identify treating on the picture and no need of the information about any camera and expansive number of picture for basic leadership. Duplicate glue forgery is the most widely recognized sort of picture forgery wherein an area from a picture is supplanted with another district from a similar picture. Another independent technique in [17] uses a decent procedure dependent on change invariant highlights. These are essentially rely upon the Trace change and accomplished by adjusting the MPEG-7 picture signature devices descriptors in numerous viewpoints. Thus this is very productive plan for picture forgery recognition.

Results and Discussion

We have examined different strategies that are proposed by different The developers of the technique to recognize picture forgery. The perspective of the significant number of methodologies is to perceive the impersonation in the image yet the techniques are differing. The accompanying table 1 demonstrates the correlation of different duplicate move forgery location techniques, which have talked about in this paper.

From the outcomes table we can distinguish that DISCRETE COSINE TRANSFORM, Wavelet, LBP and SuRF are the most widely recognized strategies utilized with the end goal of forgery identification. While wavelet based strategies have great exactness, the techniques including SuRF and SCALE INVARIANT FOURIER TRANSFORM are normally utilized for high precision applications. These techniques have higher computational deferral, however would lessen the measure of endeavors required for re-preparing the pictures because of their ideal exactness.

Technique	Correlation value
DCT	0.3
Wavelet	0.35
LBP	0.8
SuRF	0.82
SIFT	0.82

Table 1. Correlation Value of Different Techniques

Conclusion

In this paper different methods of image forgery detection have been mentioned and discussed. These methods have the capability to identify forged images. In any case, a few algorithms are not viable regarding identifying actual forged region. Moreover wavelet and SuRF based methods are the most used methods for feature extraction in the forgery detection space and thus can be used in order to improve the accuracy of detection when combined with machine learning and artificial intelligence, thus researchers can focus on that area of work in order to improve the performance of the system.

References

1.T. Chihaoui, S. Bourouis and K. Hamrouni, “Copy-move image forgery detection based on SCALE INVARIANT FOURIER TRANSFORM descriptors and SINGULAR VALUE DECOMPOSITION-matching,” 1st International Conference on Advanced Technologies for Signal and Image Processing (ATSIP), Sousse, 2014, pp. 125-129.

2. L. Yu, Q. Han and X. Niu, “Copy-Rotation-Move Forgery Detection Using the MROGH Descriptor,” IEEE International Conference on Cloud Engineering (IC2E), 2014, Boston, MA, 2014, pp. 510-513.

3. B. Xu, G. Liu and Y. Dai, “A Fast Image Copy-Move Forgery Detection Method Using Phase Correlation,” Fourth International Conference on Multimedia Information Networking and Security, Nanjing, 2012, pp. 319-322.

4 S. Ketenci and G. Ulutas, “Copy-move forgery detection in images via 2D-Fourier Transform,” 36th International Conference on Telecommunications and Signal Processing (TSP), 2013, Rome, 2013, pp. 813-816.

5 H. C. Hsu and M. S. Wang, “Detection of copy-move forgery image using Gabor descriptor,” Anti-counterfeiting, Security, and Identification, pp.1-4, Taipei, 2012.

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

6. H. Yao, T. Qiao, Z. Tang, Y. Zhao and H. Mao, "Detecting Copy-Move Forgery Using Non-negative Matrix Factorization," Third Interna-tional Conference on Multimedia Information Networking and Security, Shanghai, 2011, pp. 591-594.
7. G. Muhammad, M. H. Al-Hammadi, M. Hussain, A. M. Mirza and G. Bebis, "Copy move image forgery detection method using steerable pyra-mid transform and texture descriptor," IEEE EUROCON, 2013, Zagreb, 2013, pp. 1586-1592.
8. D. Cozzolino, G. Poggi and L. Verdoliva, "Copy-move forgery detection based on Patch Match," IEEE International Conference on Image Process-ing (ICIP), Paris, 2014, pp. 5312-5316.
9. M. Hussain, G. Muhammad, S. Q. Saleh, A. M. Mirza and G. Bebis, "Copy-Move Image Forgery Detection Using Multi-Resolution Weber Descriptors," Eighth International Conference on Signal Image Technology and Internet Based Systems (SITIS), Naples, 2012, pp. 395-401.
10. M. B. Imamoglu, G. Ulutas and M. Ulutas, "Detection of copy-move forgery using Krawtchouk moment," 8th International Conference on Electrical and Electronics Engineering (ELECO), 2013, Bursa, 2013, pp. 311-314.
11.Xiaomei Quan and Hongbin Zhang, "Copy-move forgery detection in digital images based on local dimension estimation," International Confer-ence on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), Kuala Lumpur, 2012, pp. 180-185.
12.V. Christlein, C. Riess, J. Jordan, C. Riess and E. Angelopoulou, "An Evaluation of Popular Copy-Move Forgery Detection Approaches," IEEE Transactions on Information Forensics and Security, vol. 7, no. 6, pp. 1841-1854, Dec. 2012.
13.H. Huang, W. Guo, and Y. Zhang, "Detection of copy-move forgery in digital images using SCALE INVARIANT FOURIER TRANSFORM algorithm," Pacific-Asia Workshop on Compu-tational Intelligence and Industrial Application, Vol. 2, pp. 272-6, Dec. 2008.
14.K. Sudhakar, V. M. Sandeep and S. Kulkarni, "Speeding-up SCALE INVARIANT FOURIER TRANSFORM based copy move forgery detection using level set approach," International Conference on Advances in Electronics, Computers and Communications (ICAECC), 2014, Bangalore, 2014, pp. 1-6.
15.N. Muhammad, M. Hussain, G. Muhammad and G. Bebis, "Copy-Move Forgery Detection Using Dyadic Wavelet Transform," Eighth International Conference on Computer Graphics, Imaging and Visualization (CGIV), Singapore, 2011, pp. 103-108.
16.Z. Qu, and G. Qiu, "Detect digital image splicing with visual cues," Lect. Notes Comput. Sci., Vol. 5806, pp. 247-326, Jan. 2009.
17.Z. Lin et al., "Fast, automatic and fine-grained tampered JOINT PHOTOGRAHIC EXCHANGE GROUP FORMAT image detection via DISCRETE COSINE TRANSFORMcoefficient analysis," Pattern Recogn.,Vol. 42, pp. 2492-2250, 2009.
18.M. F. Hashmi, A. R. Hambarde and A. G. Keskar, "Copy move forgery detection using DISCRETE WAVELET TRANSFORM and SCALE INVARIANT FOURIER TRANSFORM features," 13th International Conference on Intelligent Systems Design and Applications, Bangi, 2013, pp. 188-193.
19.P. Kakar and N. Sudha, "Detecting copy-paste forgeries using transform-invariant features," IEEE 15th International Symposium on Consumer Electronics (ISCE), Singapore, 2011, pp. 58-61.
20. S. A. Fattah, M. M. I. Ullah, M. Ahmed, I. Ahmmed and C. Shahnaz, "A scheme for copy-move forgery detection in digital images based on 2D-DISCRETE WAVELET TRANSFORM," IEEE 57th International Midwest Symposium on Circuits and Systems (MWSCAS), College Station, TX, 2014, pp. 801-804.

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495